SHIELDEX

APT 공격, 랜섬웨어
계속 당하고만 계시겠습니까?

차별화된 기술로 APT, 랜섬웨어 대응하는 외부유입파일관리 솔루션
외부에서 유입된 의심스런 파일을 격리/방역/감시/추적/차단하여 PC 핵심영역 보호
문서 방화벽 기술을 통해 이메일에 첨부된 악성문서를 방역하여 안전한 컨텐츠만 내부로 반입

- APT, 랜섬웨어 등 사이버 위협 증가로 국가와 산업 전반에 큰 피해 발생
- 기존의 패턴 분석, 모니터링/포렌식 방식을 회피하는 악성코드가 늘고 있는 상황
- 망분리가 도입된 환경이라도 이메일, USB, 망연계 서버로부터 유입되는 파일에 의한 공격 잠재
- 이메일 첨부파일, 웹사이트 첨부문서를 이용한 공격 방식이 늘고 있으며, 이에 대한 대응 방안 필요

SHIELDEX

- <외부인 출입보안 체계>를 네트워크 환경에 적용해 <외부유입파일 보안관리 체계>로 구현
- 이메일, USB, 망간자료전송 등 다양한 외부 경로를 통해 유입되는 모든 외부유입파일의 위협 방어

외부인 출입보안 체계

면회실
내부와 격리된 별도의 업무미팅 공간
별도의 출입증 발급 필요 없음

외부인 출입 절차
방문 접수 데스크에서 방문승인 절차 후
출입증 교부

상주 내방자 관리
CCTV, 출입증을 통한 통제, 위치 추적등의
방법을 통해 허가 받은 구역만 출입 가능

통제구역
중요 시설에 대한 관계자 외 출입금지,
외부인 출입금지 구역 설정

보안 사고 조치
경보 발생, 경비 출동하여 이상 행동을 실시한 자에
대한 색출/적발 후 퇴출

외부 유입파일 보안관리 체계

V-Room
격리된 환경을 제공하여 외부 유입파일 실행에
따른 Local System 변화를 최소화

파일유입 절차
문서/실행파일 대한 1차적 방역
외부유입파일에 대한 식별

유입파일 관리
동작 모니터링, 권한에 따른 기능 동작 허용/차단
외부 유입파일에 아이콘 표시 및 추적

R-Area
시스템 변조/파괴가 가능한 영역에 대한 통제,
악의적인 시도 시 프로세스 차단

보안 사고조치
외부 유입된 위험파일을 반입경로 및 사용자 추적
위험파일에 대해 실행차단, 삭제, 반입차단 정책 설정

기존 보안방식 한계점 보완

문서를 이용한 악성코드에 효과적 대응
망분리 환경에 특화된 기능 제공

잠재적 보안위협 최소화

다양한 경로를 통한 보안위협을 단계적으로
제거/감시하는 상시 방역시스템 구축

IT 보안체계 확립

외부유입파일 식별과 차단으로 안전한 업무환경
마련, 근본 위협원인에 대한 대응체계 확립

적용대상

01
망분리 환경에서 외부유입파일에 대한 보안강화를 고려하고 있는 조직

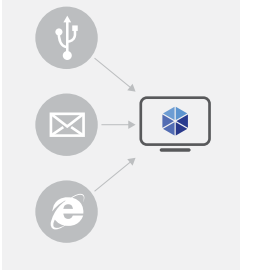
02
APT, 랜섬웨어 등 사이버 위협에 대한 대응 방안을 고려하고 있는 조직

03
ZeroDay 등 알려지지 않은 공격에 대한 강화된 보안대책 마련이 필요한 조직

04
금융/에너지/국방 등 고도화된 사이버 테러 집단의 잠재적 공격 대상 조직

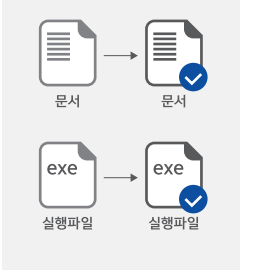
주요기능

가상격리 환경 제공 (Isolation)



격리된 환경에서 외부유입파일에 대한 안전실행모드를 제공하여 PC환경 보호

방역처리 (Sanitization)



파일 내부 반입시 방역을 통해 안전한 컨텐츠만 내부 반입

PC핵심영역 보호 (Serveillance)

외부 유입파일의 PC 중요영역 접근 감시 및 핵심영역 보호

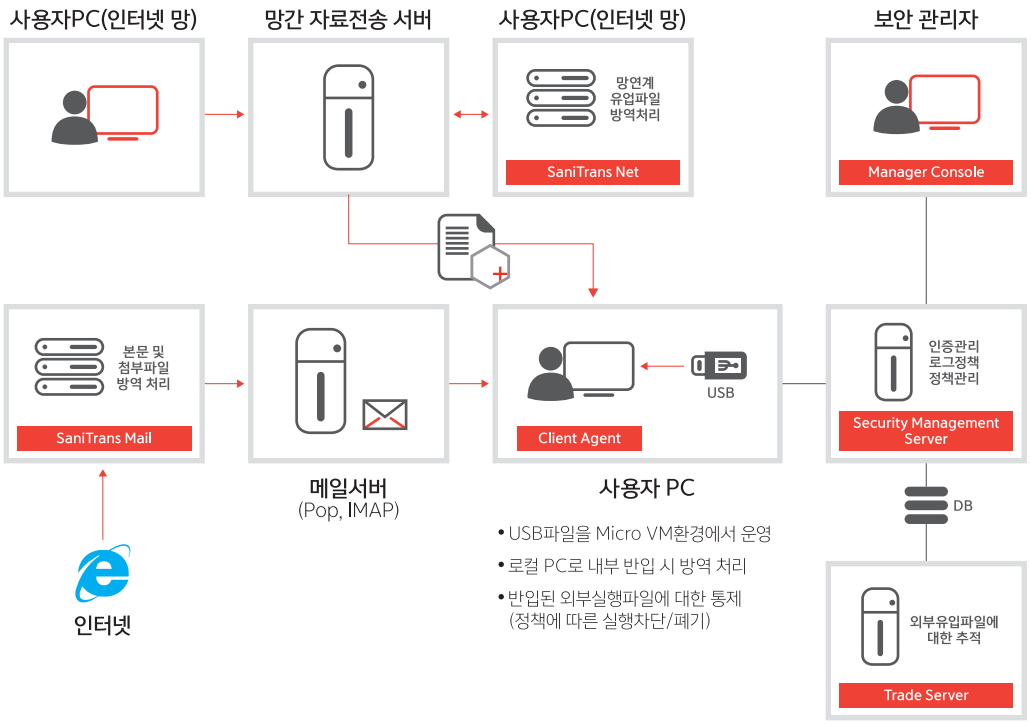
외부유입파일 통제 (Policy Control)

특정 경로(메일, USB) 및 특정 파일의 반입/실행 차단, 폐기 등 보안정책 설정

추적/현황 관제 (Trace)

외부유입파일의 사용이력 추적 및 차단현황 관제

시스템 구성도



옵션제품

Trade Server
외부유입파일 대한 추적/모니터링 관리 (차단정책 설정)

SaniTrans Net
망간자료전송시스템을 통해 내부망으로 유입되는 파일에 대한 방역 및 통제

SaniTrans Mail
외부 메일 본문 방역 및 첨부파일 방역

Client
외부 유입파일이 실환경에 영향을 끼치지 못하도록 Micro VM을 통한 가상화

외부유입파일의 이용내역 감시 및 PC핵심영역 접근차단